CLAIMS

What is claimed is:

1. A computerized method for restricting network access by applications comprising:

detecting a network access request from an application;

examining an application policy file to determine if the application is authorized to access the network; and

blocking access to the network if the application is not authorized to access the network.

2. The method of claim 1 further comprising:

determining a network resource requested by the application;

examining the application policy file to determine if the application is authorized to access the network resource; and

allowing access to the network resource if the application is authorized to access the network resource.

3. The method of claim 1 further comprising:

determining a type of network access requested by the application;

examining the application policy file to determine if the application is authorized for the type of network access requested; and

allowing the type of network access requested if the application is authorized for the type of network access requested.

4. The method of claim 1 further comprising:

updating the application policy file; and

re-evaluating applications currently executing against the updated policy file.

5. The method of claim 1 further comprising:

determining if the application is allowed access to the network based on an application identifier in the network access request.

6. The method of claim 1, wherein the method is performed on a client computer on which the application is executing.

7. A computer-readable medium having executable instruction to cause a computer to perform a method comprising:

detecting a network access request from an application;

examining an application policy file to determine if the application is authorized to access the network; and

blocking access to the network if the application is not authorized to access the network.

8. The computer-readable medium of claim 7, wherein the method further comprises:

determining a network resource requested by the application;

examining the application policy file to determine if the application is authorized to access the network resource; and

allowing access to the network resource if the application is authorized to access the network resource.

9. The computer-readable medium of claim 7, wherein the method further comprises:

determining a type of network access requested by the application;

examining the application policy file to determine if the application is authorized for the type of network access requested; and

allowing the type of network access requested if the application is authorized for the type of network access requested.

10. The computer-readable medium of claim 7, wherein the method further comprises:

updating the application policy file; and

re-evaluating applications currently executing against the updated policy file.

11. The computer-readable medium of claim 7, wherein the method further comprises:

determining if the application is allowed access to the network based on an application identifier in the network access request.

12. A computer system comprising:

a processing unit;

a memory coupled to the processing unit through a bus;

a network interface coupled to the processing unit through the bus and further operable for coupling to a network; and

an application policy process executed from the memory by the processing unit to cause the processing unit to detect a network access request from an application, to examine an application policy file to determine if the application is authorized to access the network, and to block access to the network if the application is not authorized to access the network.

13. The computer system of claim 12, wherein the application policy process further causes the processing unit to determine a network resource requested by the application, to examine the application policy file to determine if the application is authorized to access the network resource, and to allow access to the network resource if the application is authorized to access the network resource.

14. The computer system of claim 12, wherein the application policy process further causes the processing unit to determine a type of network access requested by the application, to examine the application policy file to determine if the application is

authorized for the type of network access requested, and to allow the type of network access requested if the application is authorized for the type of network access requested.

15. The computer system of claim 12, wherein the application policy process further causes the processing unit to update the application policy file, and to re-evaluate applications currently executing against the updated policy file.

16. The computer system of claim 12, wherein the application policy process further causes the processing unit to determine if the application is allowed access to the network based on an application identifier in the network access request.

17. The computer system of claim 12, wherein the application is executed from the memory by the processing unit.

18. A computer-readable medium having stored thereon an application policy data structure comprising:

an application identifier field containing data identifying an application;

a network identifier field containing data identifying a entity that is accessible by the application identified by the application identifier field; and

an access flag field containing data specifying whether the application identified by the application identifier field is allowed access to the entity identified by the network identifier field.

19. The computer-readable medium of claim 18 further comprising:

an additional policy rule field containing data specifying whether the application identified by the application identifier field is allowed a particular type of access to the entity identified by the network identifier field.

20. The computer-readable medium of claim 18 further comprising:

a response field containing data specifying an action to performed if the application identified by the application identifier field attempts access to the entity identified by the network identifier field and the access is not allowed.

21. The computer-readable medium of claim 18, wherein the entity is selected from the group consisting of a network and a network resource.